Bluetooth Security — True or False

Better Analysis™ Reveals the Myths – Explains the Science

Introduction

Bluetooth security is complex and often misunderstood. It can also be implemented incorrectly, exposing otherwise excellent designs to great risk of commercial failure. As Bluetooth has become one of the most common wireless standards in use today, understanding its security principles has become ever more important for implementers of Bluetooth technology.

Ellisys analyzers are optimized to help engineers characterize adherence to a broad range of specification requirements, including security. As well, Ellisys analyzers assist academia and other researchers in making Bluetooth more secure by helping to understand newly discovered attack scenarios or in proactively searching for new ways to circumvent Bluetooth security.

This Expert Note will cover ten often misunderstood security concepts and help users of Ellisys analyzers with an understanding of how security affects their implementation.

Take the True/False test below and see if you can answer all of them correctly.

True or False

1. All Bluetooth low energy devices after version 4.2 use LE Secure Connections pairing.

Bluetooth Low Energy devices establish connections using **LE Secure Connections** pairing (introduced in version 4.2) or **LE Legacy** pairing (introduced in version 4.0). LE Legacy pairings will use a Temporary Key (TK) that is used to create a Short-Term Key (STK), and this is used to initially encrypt the connection for purposes of distributing security keys. With LE Secure Connections, Elliptic Curve - Diffie Hellman (ECDH) cryptography is used to create a highly secure Long-Term Key (LTK), which is retained by both devices.

During the pairing process, a Features Exchange sequence is used to determine whether both devices advertise support for LE Secure Connections, and if so, SC is used, otherwise LE Legacy Pairing will be used. Answer: **False.**

HELPFUL HINT: Ellisys sniffers crack the LE Legacy pairing procedures and calculate the STK based on over-the-air traffic only.

True or False

2. Backward compatibility is always available and always enforced in Bluetooth security.

In “Secure Connections Only” mode, often called a “FIPS mode,” Bluetooth devices actually prioritize security over backward compatibility with devices that do not support this mode. This mode is enforced by the host, which can reject connection attempts when Secure Connections is not enabled. This feature is available on Bluetooth LE and on BR/EDR (as an enhancement to Secure Simple Pairing). Answer: **False.**

True or False

3. Bluetooth devices are generally most vulnerable to an attack during pairing.

Indeed, Bluetooth devices are most commonly attacked during the pairing process, when critical authentication and encryption processes take place. Successful attacks can also occur during an established connection, although this is more difficult and less common. Answer: **True.**

True or False

4. A dual-mode device may use a single pairing procedure to generate keys for both transports.

A procedure called Cross-Transport Key Derivation (CTKD) allows a device (under certain circumstances) to pair once and share a derivation of its link key from one transport to the other (BR/EDR and Bluetooth LE). This is a convenience that prevents the user from having to manage two different pairing procedures.

> HELPFUL HINT: The Ellisys Bluetooth Qualifier (EBQ) Test System actively verifies adherence to CTKD requirements, along with more than 1600 other tests.

A known key-overwrite vulnerability, called BLURTooth, uses the CTKD feature to access one transport (with lower security, like Just Works) to access services on the other transport (with higher security). An update to the Bluetooth specification adds measures to protect against this threat. Answer: **True.**

True or False

5. BR/EDR pin-code pairing is not secure.

As with LE Legacy pairing, this BR/EDR legacy pairing method does not provide any real security. While it is not as commonly implemented as it was prior to the introduction of Secure Simple Pairing (SSP), it is still used in a variety of new development and in older devices. Answer: **True.**

> HELPFUL HINT: Ellisys analyzers can automatically and passively determine a pin-code (typically 4 digits) and deduce the related link key within a few hundred milliseconds.

True or False

6. FHSS is a strong obstacle to Bluetooth attackers.

Frequency Hopping Spread Spectrum (FHSS), while useful to reduce the negative effects on the Bluetooth communication channel from ISM band interferences, is not a huge impediment to would-be attackers. The hopping sequence can be learned quickly, using only moderately sophisticated hardware and software . Answer: **False.**

HELPFUL HINT: The wideband sniffer technology pioneered by Ellisys renders FHSS completely transparent.

True or False

7. For LE Legacy pairings, only the Out-of-Band (OOB) association model protects against passive eavesdropping.

Indeed, under LE Legacy pairings, both the Just Works and Passkey Entry association models are susceptible to passive eavesdropping, while the OOB method is inherently protective against this sort of attack. For LE Secure Connections, the addition of ECDH cryptography adds protection against passive eavesdropping. Answer: **True.**

True or False

8. It is not possible for an analyzer to decrypt traffic whenever SSP or LE Secure Connections is used.

Secure Simple Pairing (BR/EDR) and LE Secure Connections, use asymmetric public key cryptography to create a secure link key (ECDH). A private key, which is not distributed and is mathematically related to the public key, is also created on each device as part of the Public/Private key “pair.” Obtaining the link key can be a challenge – it is not available unencrypted over the air, and cannot be deduced solely by capturing pairing traffic with a sniffer.

If the link key is exchanged over a host-controller interface (HCI) connection being monitored (captured) by the analyzer (e.g., UART, SPI, USB), the Ellisys software will automatically retain and apply the key to the appropriate device pair, all without any user intervention. SSP debug keys are also detected automatically and applied without user intervention as well . If available, the SSP Private Keys can be entered and stored locally for added ease of use. Answer: **False.**

True or False

9. In a Broadcast Isochronous Group (BIG), encryption is optional.

A BIG uses Security Mode 3, Levels 1, 2, or 3. In Level 2 (unauthenticated) and 3 (authenticated), the Broadcast Code is used to create keys necessary for encryption and decryption. These keys include a Group Long-Term Key (GLTK), Group Session Key (GSK), Group Session Key Diversifier (GSKD). There is no authentication or encryption in level 1. Answer: **True.**

True or False

10. A Connected Isochronous Stream (CIS) uses the same session key for encryption that is used by an associated ACL.

The master of an ACL connection, as directed by the host, can create a Connected Isochronous Stream (CIS), which is "associated" with that ACL. More than one CIS can be associated with the same ACL. If the ACL is encrypted, any associated CIS must be encrypted, and conversely, if an ACL is not encrypted, all associated CIS are also not encrypted. Answer: **True.**

Conclusion

So, what is your score? If you knew the correct answer to all topics above, please get in touch with Ellisys at the next UPF event and we'll buy you a beer, or the beverage of your choice! Either way, you should now know that while Bluetooth security is comprehensive, after learning and understanding its processes, it's actually not that complex. Here is where the Ellisys protocol analyzer can help you overcome the learning curve and implementation challenges.

Other Interesting Reading

- EEN_BT01 - Capturing Bluetooth Traffic, the Right Way
- EEN_BT03 - Your First Wideband Capture
- EEN_BT07 - Secure Simple Pairing Explained

More Ellisys Expert Notes available at:
www.ellisys.com/technology/expert_notes.php

Feedback

Feedback on our Expert Notes is always appreciated. To provide comments or critiques of any kind on this paper, please feel free to contact us at expert@ellisys.com

Sales Contact:

USA: +1.866.724.9185
Asia: +852 2272 2626
Europe: +41 22 777 77 89

sales@ellisys.com

www.ellisys.com

Connect with us.